

# FAA National Software Conference

## Previously Developed Software

### PREVIOUSLY DEVELOPED SOFTWARE

FAA SOFTWARE  
STANDARDIZATION CONFERENCE

Seattle, WA

August 8-11, 2000

Jorge Castillo - FAA/ASW-110



**"Guidelines For  
Applying DO-178B  
Level D Criteria To  
Previously  
Developed  
Software (PDS)"  
Notice N8110.82**

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Purpose & History

- **PURPOSE:**
  - To Give Guidelines For Meeting DO-178B Level D Objectives For PDS
- **HISTORY:**
  - Began When Applicant Desired To Use Windows NT On Their Airborne Equipment
  - PDS Is Big Issue For Industry
  - Routed For Comment Sept 1998
  - Signed March 1999

N8110.82

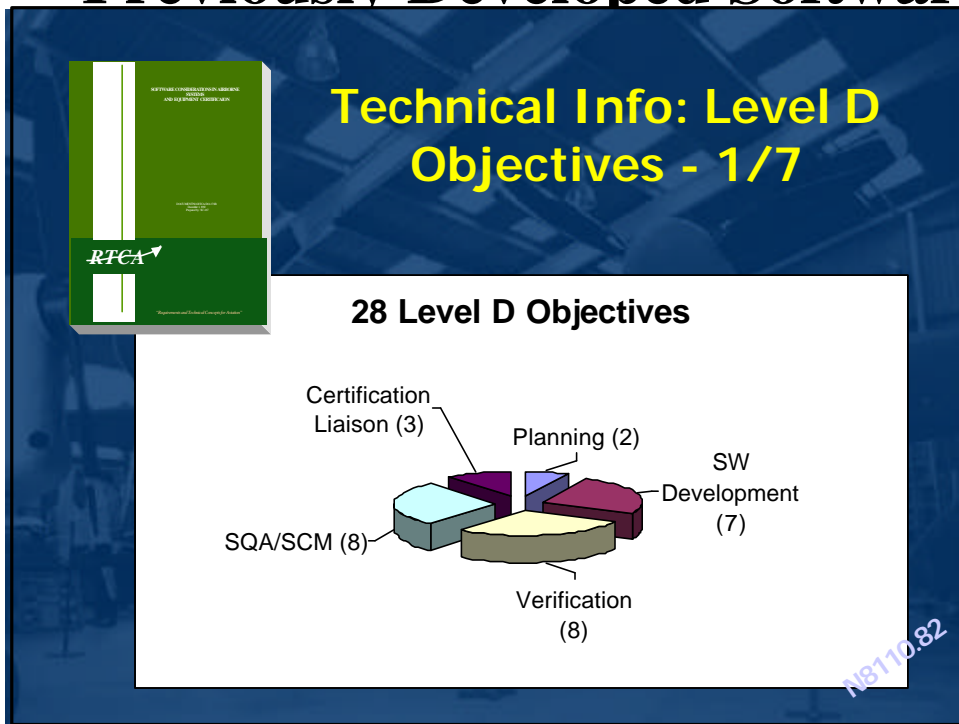
### Technical Information: What Is PDS?

- Software that was not developed using DO-178B
  - Commercial-off-the-shelf
  - Military Standards
  - Other Industry Standards
  - DO-178 or DO-178A
  - etc.



# FAA National Software Conference

## Previously Developed Software



- ### Technical Info: Level D Objectives - 2/7
- Two Planning Objectives: 1-1, 1-4
  - There Must Be a Plan (per 1-1)
    - Don't Evaluate Quality of Plan (1-6)
    - Plan May Not Meet DO-178B (1-6)
  - Plan Must Be Followed (9-1)
  - Additional Considerations Should Be In The Plan (1-4)
    - Magic
    - Service Experience
- N8110.82

# FAA National Software Conference

## Previously Developed Software

### Technical Info: Level D Objectives - 3/7

- Eight SQA/SCM Objectives
  - Plan Was Carried Out
  - Product Configuration Is Identified, Protected, And Explained
  - What Is Approved Is What Is Flying

N8110.82

### Technical Info: Level D Objectives - 4/7

- Three Certification Liaison Objectives:
  - Cert Authority Agreement Up Front
  - Data In Place To Prove:
    - Plan Was Followed
    - DO-178B Objectives Were Met

N8110.82



# FAA National Software Conference

## Previously Developed Software

### Technical Info: Level D Objectives - 5/7

- Eight Verification Objectives
  - Six Concentrate on Functional Testing
    - High Level Req Good & Trace to Sys Req
    - Executable Complies and Is Robust With High Level Req
  - One Verifies Behavior of Object Code in Target Environment
    - Executable Code Compatible w/ Target Computer
  - One Verifies That Partitioning Is Not Compromised

N8110.82

### Technical Info: Level D Objectives - 6/7

- Seven Development Objectives: Table A-2
  - 2-1: High Level Req Developed
  - 2-2: Derived High Level Req Are Defined
  - 2-3, 2-4, 2-5: SW Architecture/Low Level Req Are Developed
    - ... From High Level Req
    - No Verification Objectives Cover This

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Technical Info: Level D Objectives - 7/7

- Seven Development Objectives (cont)
  - 2-6: Source Code Is Developed
    - ... Traceable to and Conforms with Low Level Req
    - No Verification Objectives Cover This
  - 2-7: Object Code is Produced and Executes in Target Computer
    - No Verification Objectives Cover This
    - High Level Req Testing Subsumes This

N8110.82

### Notice Outline

- 7 Sections:
  - Section 1: Purpose
  - Section 2: Distribution
  - Section 3: Related Publications
  - Section 4: Background
  - Section 5: Discussion
  - Section 6: Procedures
  - Section 7: Conclusion

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Background (Section 4) - 1/2

- Level D to Address a Minor Aircraft Failure Condition
- Level D Intended to Provide a Thorough Investigation of the Functional Behavior of the Software
- Level D Intended to Provide the Necessary Configuration Control

N8110.82

### Background (Section 4) - 2/2

**28**  
**objectives**

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Discussion (Section 5)



### 5 Confusing Objectives

1-1, 2-3, 2-4, 2-5, 2-6

N8110.82



### Objective 1-1 (Section 5a)

- 1-1, "Software Development and Integral Processes Activities are Defined," Req'd for Level D
- 1-6, "Software Plans comply with this document," Not Req'd For Level D
- Interpretation:
  - There Must Be Plans (1-1)
  - Plans Should Assure SW Meets DO-178B Objectives
  - Plans Must Be Followed (9-1)

N8110.82



# FAA National Software Conference

## Previously Developed Software

### Objective 2-4 (Section 5b)

- 2-4: "Low-level Requirements Are Developed"
- Intent: Design Is Defined
- No Explicit Verification of Low Level Req or Architecture In Table A-4
- 2-4 Is Implicitly Satisfied By 6-1 & 6-2
- No Need To Assure Low Level to High Level Req Traceability for Level D PDS

N8110.82

### Objective 2-3 (Section 5c)

- 2-3: "Software Architecture Is Developed"
- Same Logic As Objective 2-4
- No Explicit Verification Activities
- Implicitly Satisfied By Other Objectives
  - I.e., 4-8 through 4-12

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Objective 2-5 (Section 5d)

- 2-5: "Derived Low-Level Requirements Are Defined"
- No Explicit Verification of Derived Low-Level Requirements
- Implicitly Satisfied By Meeting Objective 2-2 and Associated Verification of High Level Requirements

N8110.82

### Objective 2-6 (Section 5e)

- 2-6: "Source Code Is Developed"
- No Explicit Verification of Source Code In Table A-5
- Need: Exe Code to High Level Req Traceability
- Don't Need: Source Code to Low-Level Req to High-Level Req Traceability
- Interpretation: Exe Code to Meet All Functional Verification Requirements By Other Objectives

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Procedures (Section 6)

- a) Table A-2, objectives 3,4,5,6 are Implicitly Covered by Other Objectives
- b) Partitioning/Protection for Systems with Multiple Function
- c) May Need to Limit Software Level for PDS in Systems with Multiple Functions

N8110.82

### Example - 1/4

- A Company Recently Received A TSO Approval On A System Using Windows NT
- The System Was A Level C Moving Map/ Navigation Device
- However, Windows NT Was Only Approved To Level D
- Required Protection Between System (Level C) And Windows NT (Level D)
- Windows NT Was Shown To Provide Only a Minor Failure Condition

N8110.82

# FAA National Software Conference

## Previously Developed Software

### Example - 2/4

- Protection Argument Required Applicant To Demonstrate:
  - No Failure of Windows NT Can Contribute to Anything Greater Than a Minor Hazard
  - OR
  - No Failure of NT Can Affect Other Programs

N8110.82

### Example - 3/4

- Three Choices For Windows NT Approval To Level D
  - Meet Objectives for Level D
  - Sublimate as Part of Architecture
  - Service Experience

N8110.82



# FAA National Software Conference

## Previously Developed Software

### Example - 4/4

- SUMMARY OF EXAMPLE:
  - Moving Map/Navigation Device - Can Produce a Major Hazard
  - Windows NT Was Shown to Produce Only a Minor Failure Condition
    - By Considering Loss of Function vs Corruption of Function
    - By Converting all Windows NT Problems to Loss of Function
  - Windows NT is NOT Level C

N8110.82

### SC-190/WG-52's Activities

- SC-190/WG-52 Addressing PDS
  - Started As: "COTS" Sub-group
  - Became: "PDS" Sub-group
  - Now: "Development" Sub-group
- Writing Frequently Asked Questions (FAQs) and Position Papers To Clarify DO-178B

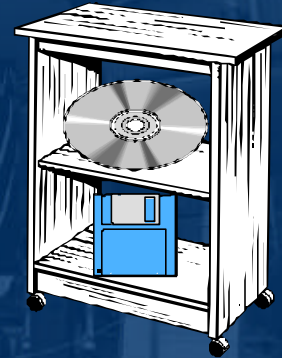
N8110.82

# FAA National Software Conference

## Previously Developed Software

### COTS Research Project

- AIR-130 Sponsoring a Research Project On COTS Hardware and Software
- Goals: Develop Criteria And Tutorial For COTS Use In Aviation Systems



N8110.82